

Seguridad en la Internet de las cosas:

Firmwares, vulnerabilidades y riesgos en la rapidez del desarrollo y consumo de Internet Of Things



UNIVERSITAT ROVIRA I VIRGILI



Álvaro Calvo del Olmo

Tutor: Carlos Hernández Gañán

Estructura de la presentación

1. Introducción
2. Análisis de dos dispositivos
3. Comunicaciones seguras
4. Routers y dispositivos de gestión
5. Los dispositivos analizados en Internet
6. Soluciones
7. Conclusiones

1.

Introducción

*Que es un IOT y su
alcance en la sociedad*



“

El IOT o Internet de las cosas es un nuevo concepto basado en la conexión de objetos de nuestro día a día a Internet

1. INTRODUCCIÓN

¿Que es un IOT?

Características que definen a un IOT:

- Conectan cosas en vez de personas
- Software muy dependiente del hardware
- Capacidades de procesamiento y memoria limitadas

Ejemplos:

- Frigoríficos
- Termostatos
- TVs
- Iluminación

1. INTRODUCCIÓN

Problemas conocidos de los IOTs

Algunos de los problemas conocidos:

- Desarrollo rápido de su software
- Soporte del fabricante demasiado corto
- Seguridad demasiado débil que, en muchos casos, no evita las contraseñas por defecto
- Exceso de exposición de los IOTs a Internet

“

El IIOT o Internet de las cosas Industrial relacionados con maquinaria, sistemas industriales, robots industriales, sensores ambientales, etc.

1. INTRODUCCIÓN

¿Donde se encuentran los IIOT?

Por la naturaleza del Industrial IIOT nos lo podemos encontrar en:

- Fábricas
- Entornos industriales
- Centrales nucleares
- Depósitos de combustible
- Estaciones meteorológicas
- ...

1. INTRODUCCIÓN

Un ejemplo de IOT:
Termostato inteligente

The screenshot shows a web browser window with the URL `8089/schedule.shtml`. The page title is "Thermostat - Setb". The interface is for a device labeled "NT120h".

Navigation Menu:

- STATUS & CONTROL
- GENERAL SETTINGS
- SETBACK SCHEDULES (highlighted in red)
- USAGE COUNTERS
- PASSWORD SETTINGS

Setback Scheduling

Day Class Schedules

Period	Time	Occupied		Unoccupied			Other		
		Heat	Cool	Time	Heat	Cool	Time	Heat	Cool
Morn	5:15 am	64.0	80.0	6:00 am	62.0	85.0	6:00 am	55.0	77.0
Day	9:00 am	64.0	78.0	8:00 am	62.0	85.0	8:00 am	70.0	77.0
Eve	9:45 pm	64.0	78.0	5:00 pm	62.0	85.0	5:00 pm	55.0	77.0
Night	11:00 pm	64.0	80.0	10:00 pm	62.0	85.0	10:00 pm	55.0	77.0

Default Weekly Schedule

Sun	Mon	Tue	Wed	Thu	Fri	Sat
Occup	Occup	Occup	Occup	Occup	Occup	Occup

[Edit Weekly Schedule](#)

Calendar View

December 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

[Goto month](#) | December | 2018

[Edit Special Days](#)

1. INTRODUCCIÓN

Un ejemplo de IIOT:
Depósitos de combustible

Depósito de combustible de una gasolinera española:

I20100

16-12-18 7:45



INVENTARIO EN TANQUE

PRODUCTO	TANQ	VOL	VOL CT	POR LL	ALTURA	AGUA	TEMP
1	GASOLEO C	19693	19719	31306	1029.0	0.0	13.60
2	GASOLEO B2	6396	6408	44603	466.3	0.0	13.22
3	GASOLEO A	21048	21048	29951	1081.1	0.0	15.58

“

*Una **Botnet** es una red de dispositivos informáticos infectados donde la persona involucrada controla de manera remota para hacer aquello que desee.*

1. INTRODUCCIÓN

¿Que es una botnet?

- Dispositivos que pueden fácilmente tener vulnerabilidades o debilidades de seguridad
- La utilidad para cibercriminales de tener algo a su servicio para realizar:
 - Ataques de Denegación de Servicio Distribuido
 - Envío de Spam
 - Minado de Bitcoins
 - Etc.

1. INTRODUCCIÓN

Botnet Mirai

- Botnet Mirai: famosa por sembrar el caos en Internet en el suceso del 21 de octubre de 2016
- Se atacó un servicio estratégico: servidores de DNS de Dyn
- Dyn es proveedor para distintas empresas que dan servicios conocidos
- Algunos de los servicios afectados: Amazon, Electronics Arts, GitHub, Netflix, Spotify...

2.

Análisis de dos IOT

Análisis en busca de vulnerabilidades y defectos de configuración



2. ANALISIS DE DOS IOT

- Análisis del firmware en modalidad de caja blanca para un reproductor multimedia con WIFI.
- Análisis de un amplificador de audio con WIFI en modalidad de caja negra.

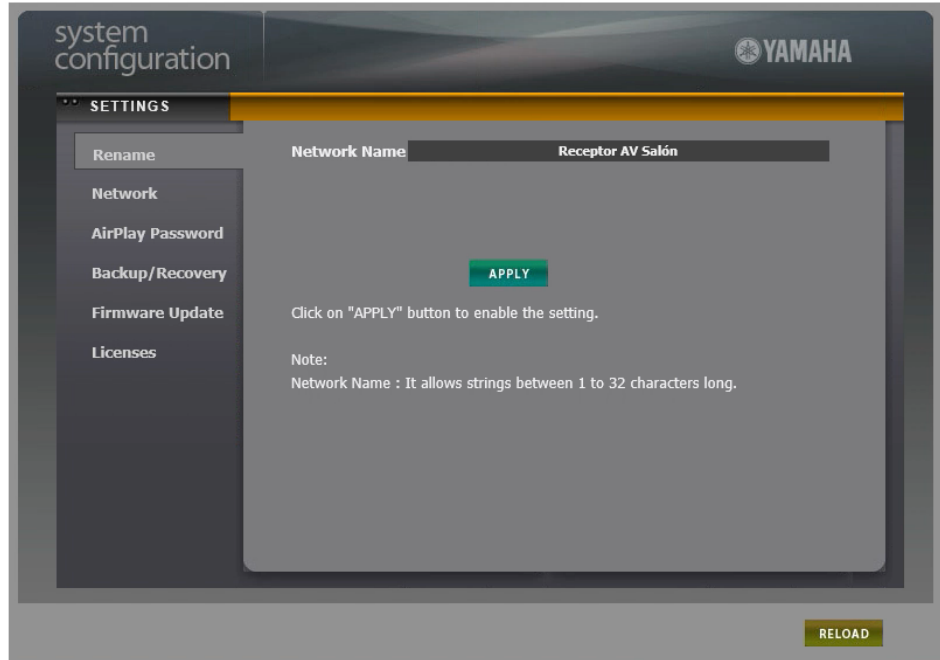
**AMBOS DE CONOCIDOS
FABRICANTES**

VIDEOS DE PRUEBAS DE CONCEPTO DEL REPRODUCTOR MULTIMEDIA

2. ANALISIS DE DOS IOT

Amplificador de audio

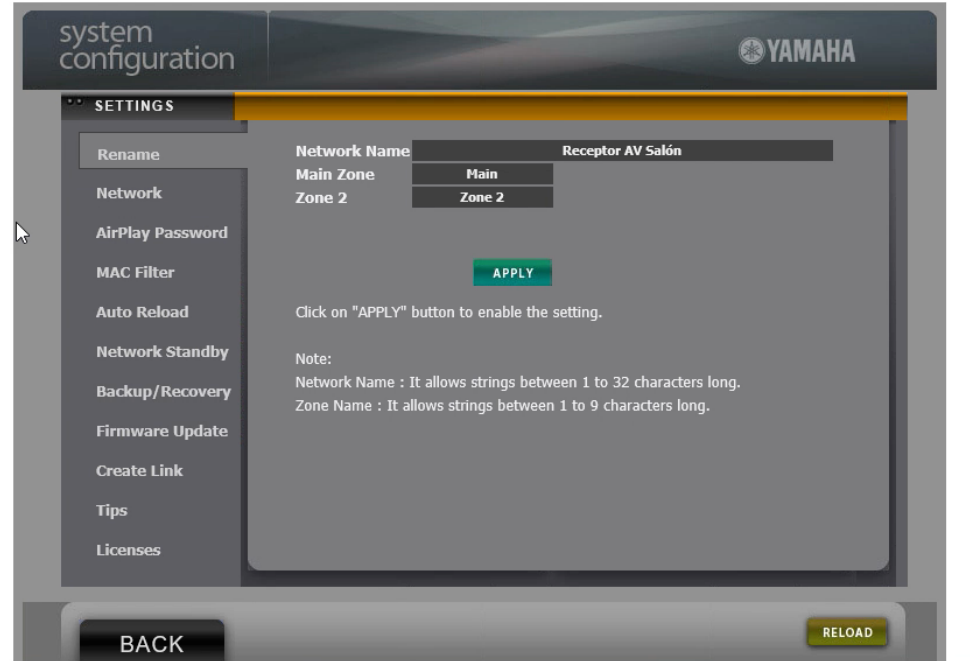
- Panel web trasero sin usuario y contraseña solo protegido por filtrado MAC
- Este panel trasero muestra mas o menos opciones de seguridad en función de la categoría del dispositivo.
- Nuestro dispositivo de pruebas es considerado de gama baja:



2. ANALISIS DE DOS IOT

Amplificador de audio

- Panel web trasero sin usuario y contraseña solo protegido por filtrado MAC
- Este panel trasero muestra mas o menos opciones de seguridad en función de la categoría del dispositivo.
- Nuestro dispositivo de pruebas es considerado de gama baja:



2.

ANALISIS DE DOS IOT

Amplificador de audio

- Panel trasero donde se puede controlar todo lo que se puede desde el mando a distancia
- Sin usuario y contraseña, solo filtrado MAC
- El panel utiliza una API compartida con la app móvil llamada YNC
- Cada opción tiene una llamada vía API que puede servir para hacer nuestros propios scripts para tener el control total de sus opciones

AV RECEIVER - Web Setup (Network) Top Menu

Power Volume Input/Output Scene Surround Speaker Sound/Video Video Adjustment HDMI
Source Device Multi Zone Trigger Out Network Display Advanced Setup Memory Guard Model Information

* Click [R] to refresh its status.

- YAMAHA_AV

- **System**
 - **Misc**
 - Network
 - Network_Standby [R] On Off On Auto
 - DMC_Control [R] Disable Disable Enable
 - Network_Name [R] Receptor AV Salón -> 1 to 32 Char
 - Product_PIN [R] AVRApple ->
 - Set**
 - YNCA_Port [R] 50000 50000 to 65535 / 1step **Set** *Click on **RESTART** to enable the change.
 - Bluetooth [R]
 - Mode On Off On
 - Send

2.

ANALISIS DE DOS IOT

Amplificador de audio

- Existencia de una API (YNCA) vía Telnet para hacer muchas de las cosas que con la app móvil
- Existencia de una tercera API que también tiene funciones duplicadas (YXC)
- Sobre esta ultima API YXC nos permite averiguar la dirección MAC del dispositivo
- El login en vtuner.com puede realizarse con la dirección MAC del dispositivo lo que permite suplantar la identidad en el servicio

```
← → ↻ ⓘ No es seguro | [IP] /Yamaha  
{ "response_code": 0, "network_name": "Yamaha",  
  "mask": "255.255.255.0", "default_gateway": "192.168.1.1",  
  "wireless_lan": { "ssid": "Yamaha", "type": "mixed_mode",  
    "type": "none", "key": "" }, "musiccast_network":  
  { "ready": false, "device_type": "unknown", "child_number": 1,  
    "wired_lan": "00A0871C0000", "wireless_lan": "00A0871C0000",  
    "irplay_pin": "" }
```

The screenshot shows the vtuner.com website. At the top right, there is a 'Logout' link and a 'STATUS' box containing: '43583 Stations Available', '9293 Podcasts', and links for 'New Stations', 'Create Account', and 'Login'. Below this is a navigation bar with 'Browse by Format, Location or Language' and sub-links for 'Browse Stations by Format', 'Browse Stations by Location', 'Browse Stations by Language', 'Browse Podcasts by Format', and 'Browse Podcasts by Location'. The main content area is a table of stations:

Station Name	Location	Genre	Stream
Eska Party	Internet Only	Dance	MP3 128K
A-1 Christmas Classical	Internet Only	Holiday	MP3 128K

VIDEO DE BLOQUEO DE VOLUMEN DE AMPLIFICADOR EN RED LAN

YAMAHA NATURAL SOUND AV RECEIVER RX-S601

VIDEO DE BLOQUEO DE VOLUMEN DE AMPLIFICADOR EN RED LAN

PHONES YPAO MIC STRAIGHT PROGRAM SCENE BD/DVD TV NET RADIO
SILENT CINEMA (CONNECT) AUX AUDIO

3.

Comunicaciones seguras

Evitar que nos espíen el tráfico



3. COMUNICACIONES SEGURAS

Uso de HTTPS

- Sobre HTTPS...
 - Muchos IOTs o no soportan HTTPS o lo soportan parcialmente.
 - Quienes lo soportan parcialmente, no permiten cargar un certificado propio.
 - Muchos IOTs no permiten ni regenerar el certificado autofirmado

3. COMUNICACIONES SEGURAS

Uso de HTTPS

- El amplificador: no soporta HTTPS.
- El reproductor multimedia :
 - Tiene integrada la misma clave privada para todas las unidades del mismo modelo.
 - Se puede extraer la clave privada del firmware e intervenir las comunicaciones de todas las unidades vendidas.

SMPP
SMRSE
SMTP
SMUX
SNA
SNMP
Snort
Socks
SoulSeek

Secure Sockets Layer

RSA keys list

SSL debug file

Reassemble SSL records sp

Reassemble SSL Application

SSL Decrypt

IP address	Port	Protocol	Key File
192.168.1.188	443	http	/media/root/SAMSUNG/certificados_https_wdtv

```
| 30 33 30 03 30 38 38 30 34 03 34 33 03 03 30 33 | -30e00004e430003 |
| 38 35 65 31 39 65 66 38 35 32 63 62 61 65 32 35 | 85e19ef852cbae25 |
| 32 3b 20 6c 61 6e 67 75 61 67 65 3d 34 3b 20 6f | 2; language=4; o |
| 6e 6c 69 6e 65 3d 31 3b 20 41 67 72 65 65 4c 69 | nline=1; AgreeLi |
| 63 65 6e 73 65 3d 31 3b 20 6b 65 65 70 53 69 67 | cense=1; keepSig |
| 6e 3d 31 0d 0a 0d 0a 70 61 73 73 77 6f 72 64 3d | n=1....password= |
| 70 61 73 73 77 6f 72 64 54 46 4d 04 f0 06 fc c1 | passwordTFM.... |
| 83 51 38 d3 44 50 f4 81 fe 3c af 13 a2 86 14 00 | .Q8.DP...<..... |
```

ssl_decrypt_record found padding 0 final len 639

checking mac (len 619, version 301, ct 23 seq 2)

tls_check_mac mac type:SHA1 md 2

Mac F201

3. COMUNICACIONES SEGURAS

Vulnerabilidad Krack

- La vulnerabilidad Krack afecta a redes WIFI con WPA/WPA2.
- Las versiones de wpa_supplicant en Linux y Android por debajo de la versión 2.3 son vulnerables a Krack.

2.

ANALISIS DE DOS IOT

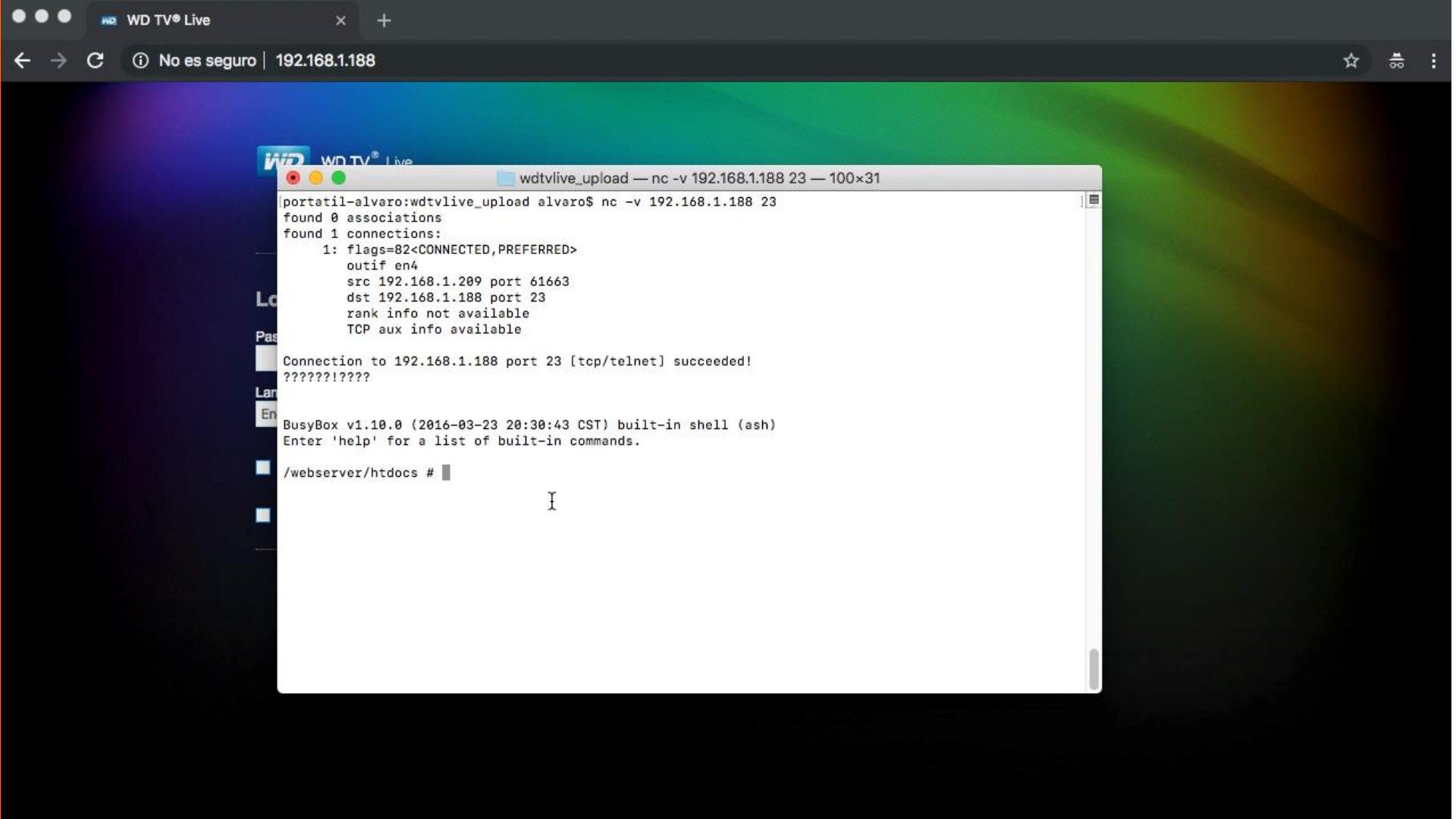
Reproductor multimedia con WIFI

```
wdtlive_upload — nc -v 192.168.1.188 23 — 100x31
RX bytes:15013501 (14.3 MiB) TX bytes:15013501 (14.3 MiB)

wlan0  Link encap:Ethernet HWaddr 00:90:A9:C1:73:DC
inet addr:192.168.1.188 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST NOTRAILERS RUNNING MULTICAST MTU:1500 Metric:1
RX packets:11403 errors:0 dropped:84 overruns:0 frame:0
TX packets:7192 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:2819908 (2.6 MiB) TX bytes:1050828 (1.0 MiB)

wlan1  Link encap:Ethernet HWaddr 02:90:A9:C1:73:DC
UP BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:6820 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)

/webserver/htdocs # ^[[A^[[A
/webserver/htdocs # ps w | grep wpa_supplicant
1429 root    37924 S    wifi_direct_manager -i wlan1 -s /etc/p2p-action.sh -c /tmp/wpa_supplicant/
-x xWIFI_DIRECT='1'
1722 root    4880 S    /usr/local/bin/wpa_supplicant.realtek -P /tmp/wpa_supplicant.pid -D nl8021
1 -B -i wlan0 -c /tmp/wpa_suppli
1829 root    4880 S    /usr/local/bin/wpa_supplicant.realtek -i wlan1 -D nl80211 -c /tmp/WFD.conf
-P /tmp/wpa_supplicant_p2p.pid
4718 root    3504 S    grep wpa_supplicant
/webserver/htdocs # /usr/local/bin/wpa_supplicant.realtek -v
/usr/local/bin/wpa_supplicant.realtek -v
wpa_supplicant v2.0-devel
Copyright (c) 2003-2012, Jouni Malinen <j@w1.fi> and contributors
/webserver/htdocs # wpa_supplicant
```



4.

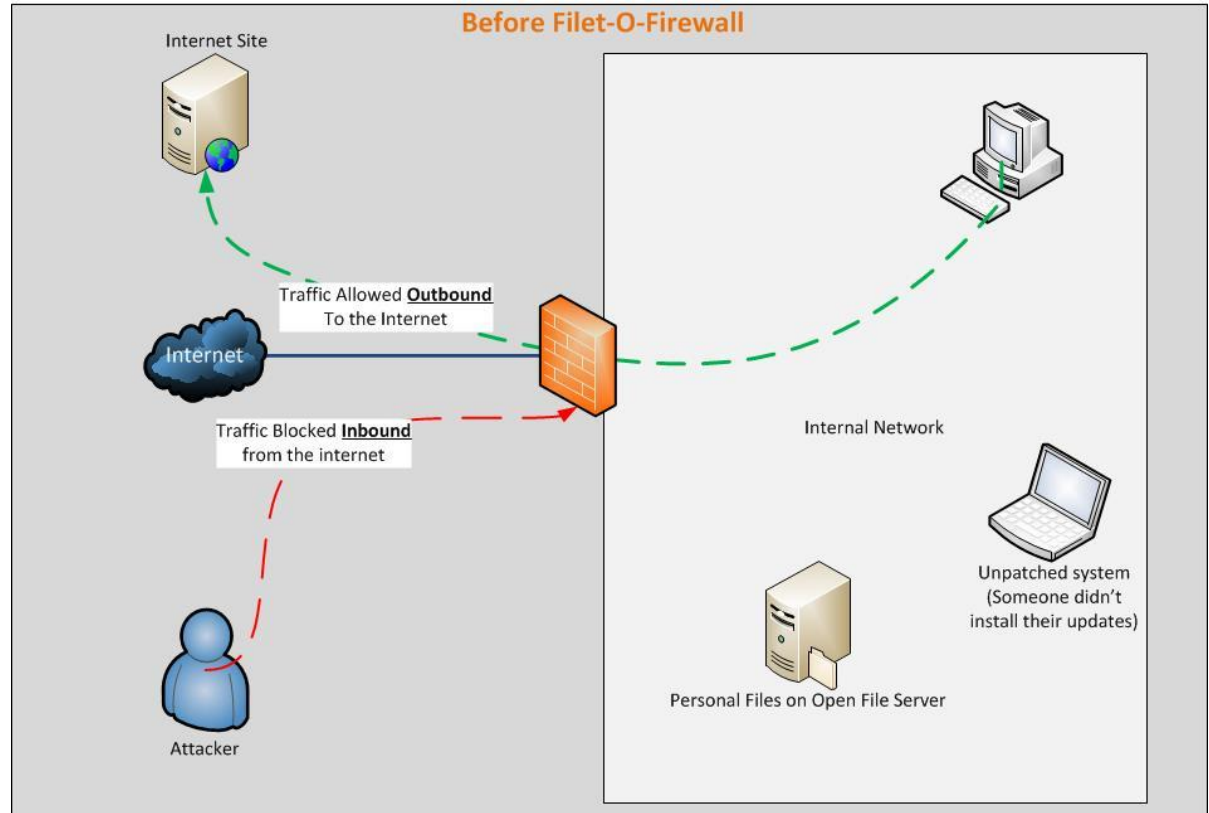
Routers y dispositivos de gestión

Los alrededores de un IOT son fundamentales



4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall



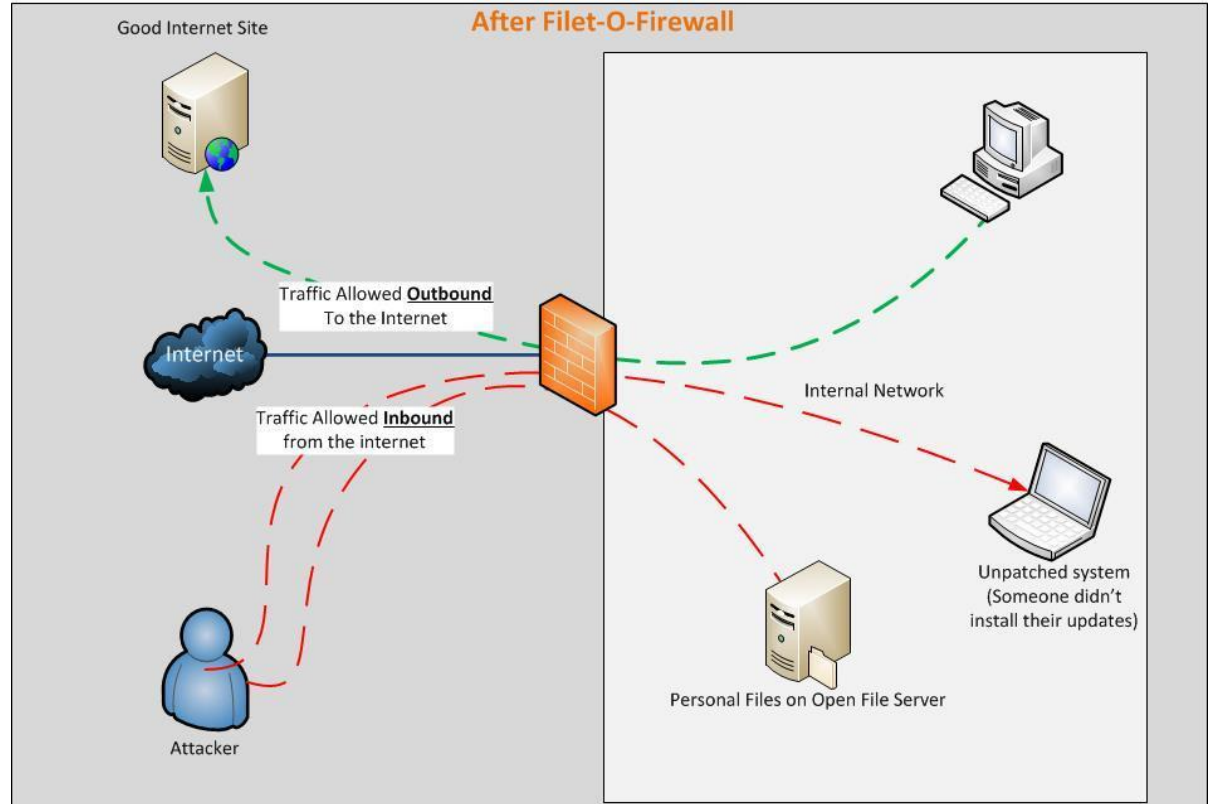
4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall

- Permitir conexiones entrantes desde Internet mediante la apertura de puertos es algo tedioso para personas no entendidas
- Gracias a IGD, un protocolo que permite que un dispositivo de la LAN “negocie” con el router la apertura automática de puertos, damos una facilidad al usuario.
- Sin embargo, IGD tiene ciertas debilidades que permiten que un programa o dispositivo no autorizado pida la apertura de puertos.

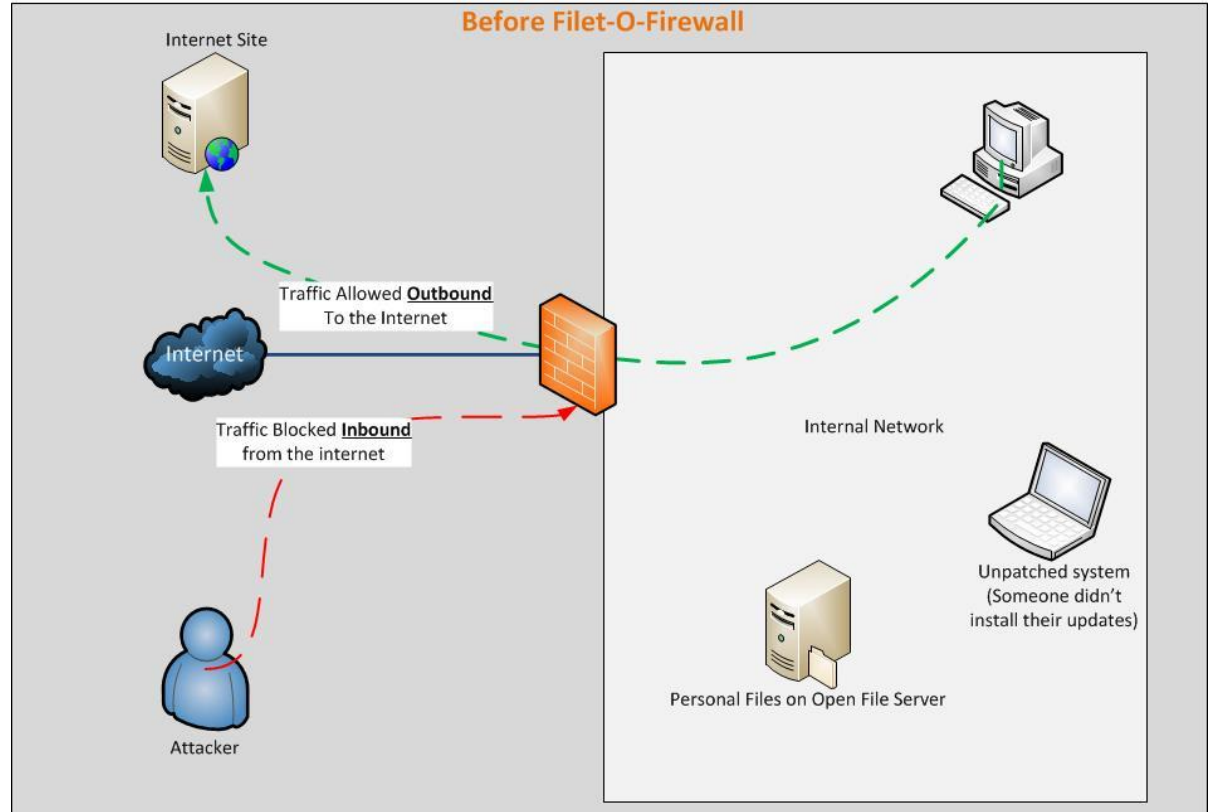
4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall



4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Filet-O-Firewall

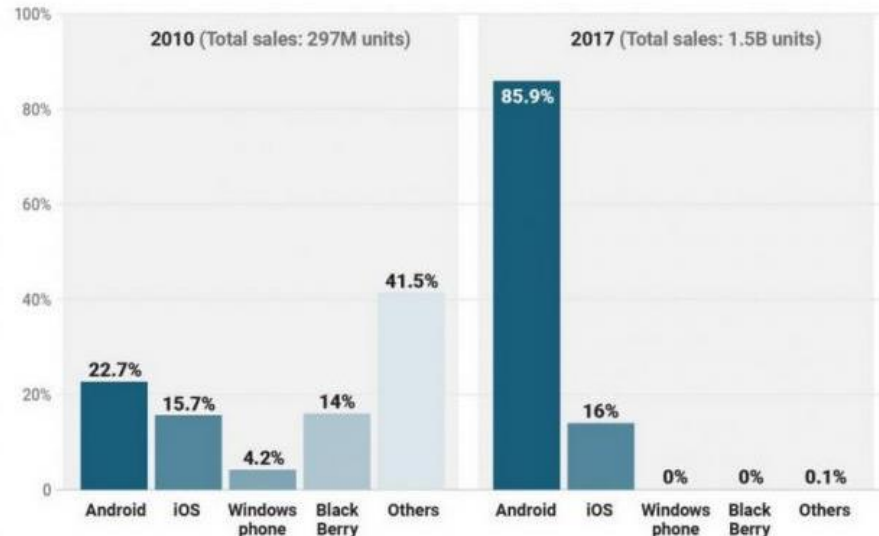


4. ROUTERS Y DISPOSITIVOS DE GESTIÓN

Sistemas operativos

- Sistemas operativos de ordenadores personales tienen ciclos de actualización mas frecuentes y con un alcance mas amplio.
- Sistemas operativos móviles (Android, iOS, etc.) tienen ciclos mas bajos de actualización, y sin embargo, son mas utilizados para manejar IOTs.

Worldwide smartphone market share by operating system



5.

Dispositivos analizados en Internet

Buscando explicaciones



5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

TOTAL RESULTS

4,841

TOP COUNTRIES



United States	1,084
Canada	727
United Kingdom	560
France	267
Netherlands	186

5. DISPOSITIVOS ANALIZADOS EN INTERNET

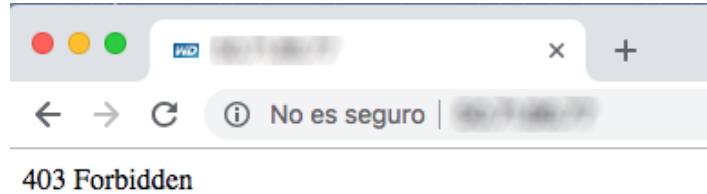
Reproductor multimedia

- Para el reproductor multimedia hubo unas decenas de IPs coincidentes con Mirai.

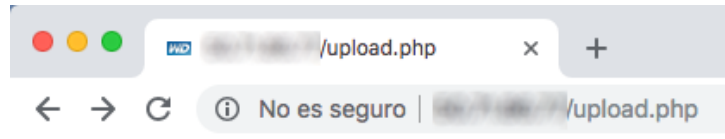
5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

- Cuando se accede desde una IP externa al reproductor multimedia, el firmware lo bloquea:



- Sin embargo upload.php no tiene esa protección, como ya sabíamos, y permite subir ficheros sin autenticación:



5. DISPOSITIVOS ANALIZADOS EN INTERNET

Reproductor multimedia

- Bajo esta situación para el usuario no tiene ningún beneficio abrir el puerto al reproductor multimedia al no aportar funcionalidad.
- Sin embargo, se ha visto muchas IPs en las que upload.php no existe, es como si algo hubiese eliminado el script para no permitir subir código PHP

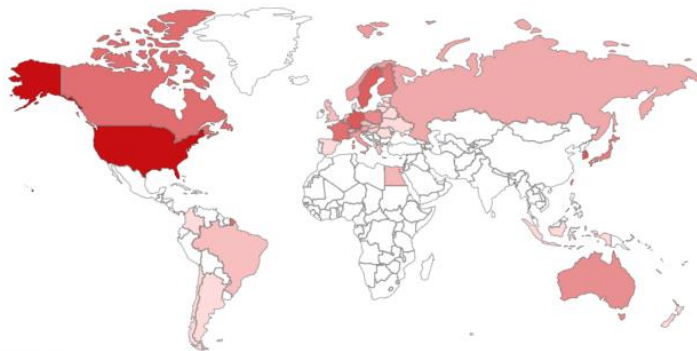
5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

TOTAL RESULTS

560

TOP COUNTRIES

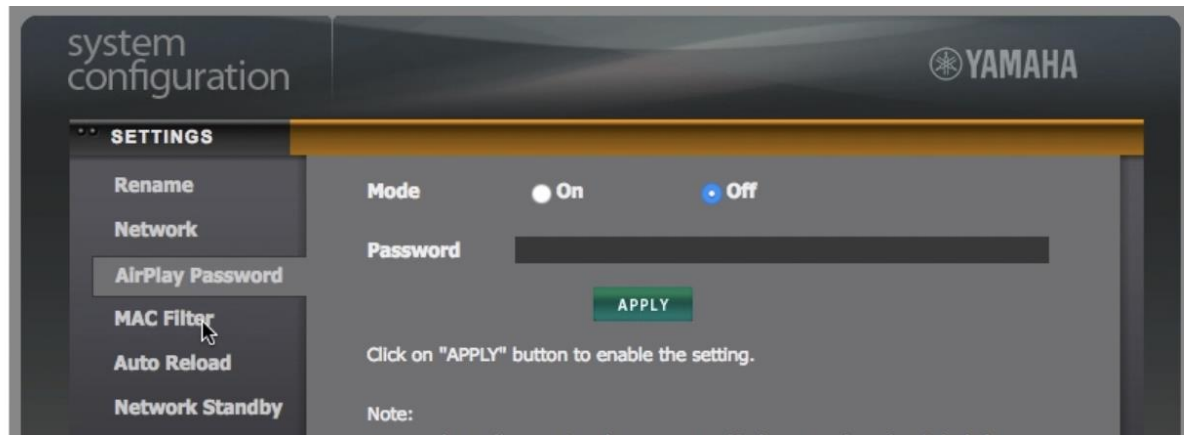


United States	173
Korea, Republic of	48
Germany	45
Sweden	41
Canada	29

5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

- Ninguna IP está implicada con Mirai.
- Todo apunta a que se han abierto los puertos a propósito para poder manejar el amplificador.
- Muchas de las IPs tienen abierto el puerto 5000 que permitiría el control de *Airplay* desde el exterior...
- ... donde la configuración expone que *Airplay* está además sin contraseña.



5. DISPOSITIVOS ANALIZADOS EN INTERNET

Amplificador de audio

- Facilidad de suplantar la identidad del dispositivo en vtuner.com a través de la dirección MAC
- Exposición del menú setup sin autenticación:

RX-A3070 - Web Setup (Advanced Setup) [Top Menu](#)

Power Volume Input/Output Scene Surround Speaker Sound/Video Video Adjustment HDMI
Source Device Multi Zone Trigger Out Network Display Advanced Setup Memory Guard Model Information

*Click [R] to refresh its status.

YAMAHA_AV
- System
- Misc
- Advanced_Setup

- Speaker_Impedance [R] 8 Ohm MIN 6 Ohm MIN 8 Ohm MIN *Click on RESTART to enable the change.
- Remote_Sensor [R] On Off On *Click on RESTART to enable the change.
- Remote_Control_ID [R] ID1 ID1 ID2 *Click on RESTART to enable the change.
- Initialize [R] Cancel Cancel Video All *Click on RESTART to enable the change.
- TV_Format [R] PAL NTSC PAL *Click on RESTART to enable the change.
- HDMI_Monitor_Check [R] Yes Yes Skip *Click on RESTART to enable the change.
- HDMI_4K_Mode [R] Mode 1 Mode 1 Mode 2 *Click on RESTART to enable the change.
- DTS_Mode [R] Mode 1 Mode 1 Mode 2 *Click on RESTART to enable the change.

VIDEO DE BLOQUEO DE VOLUMEN DE AMPLIFICADOR DESDE INTERNET

VIDEO RECEIVER RX-5601

NET RADIO
Jazz 4 Ever

-40.0



PHONES



BLUETOOTH

VIDEO MIC



STRAIGHT



(CONNECT)

PROGRAM



BD/DVD



TV



SCENE

NET



RADIO



AUX



AUDIO

6.

Soluciones

Las VPNs pueden ser parte de la solución



6. SOLUCIONES

VPN

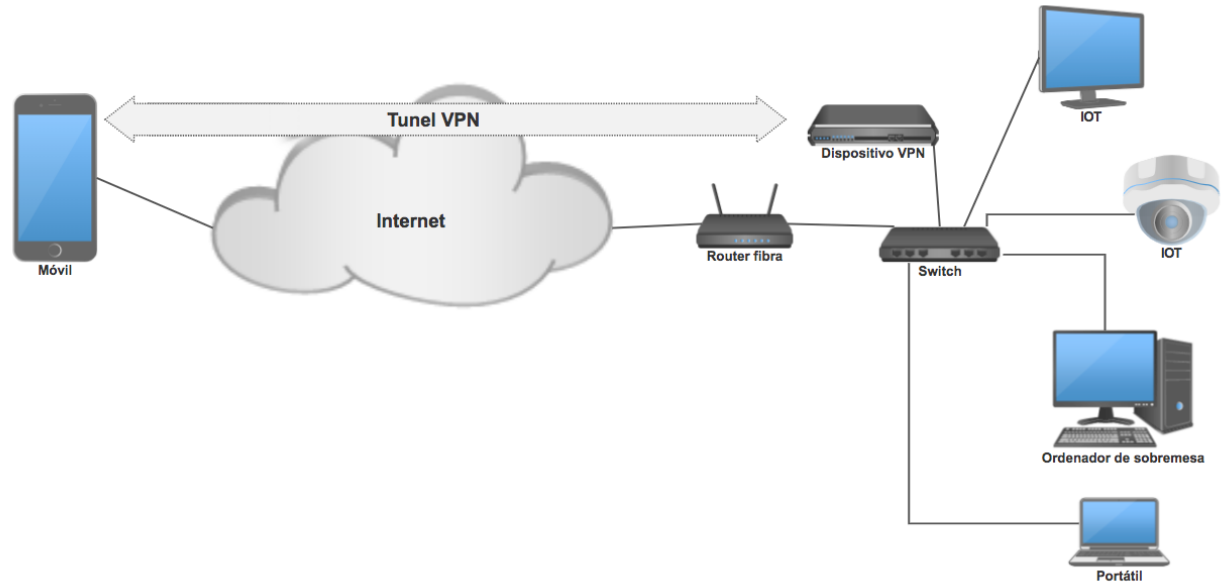
- Uso de HTTPS siempre que sea posible para preservar las comunicaciones dentro de la red LAN
- No abrir puertos que expongan el IOT directamente al exterior....

USAR VPN

- Evitamos así que se explote cualquier vulnerabilidad del IOT directamente expuesto a Internet

6. SOLUCIONES

VPN



6. SOLUCIONES

VPN

- Con VPN los accesos desde el exterior están mejor asegurados evitando que se intercepte tráfico y credenciales de IOTs, sea cual sea la red que usemos.
- Se puede combinar perfectamente con seguridad adicional como HTTPS en el IOT, ambas formas se complementan.
- Se puede preparar un servidor VPN de IOT en Raspberry Pi a muy bajo coste donde mantenerlo actualizado.



7.

Conclusiones



7. CONCLUSIONES

- Escasez de estándares y normativas que regulen las obligaciones de los fabricantes acerca del soporte máximo en tiempo en actualizaciones, las responsabilidades y estándares mínimos de seguridad.
- Falta de concienciación a los usuarios en cuanto a configuración de IOTs.
- Los fabricantes necesitan mejorar en los IOTs una configuración de seguridad fácil a los usuarios, y no ser el usuario el que tenga que investigarlo.
- Ausencia de opciones de HTTPS para proteger las comunicaciones con IOTs

7. CONCLUSIONES

- Falta de medidas para retirar dispositivos que son declarados vulnerables sin solución



7. CONCLUSIONES

- Ausencia de mejor soporte en los sistemas operativos de los dispositivos móviles
- Falta de popularización de medidas como VPN que permitan tener una red privada entre nuestro hogar y nuestro Smartphone

7. CONCLUSIONES

- Se ha demostrado la facilidad para explorar los firmwares, tanto desde la perspectiva de caja blanca como de caja negra.
- Se ha comprobado el nivel de exposición de nuestra privacidad y nuestra seguridad personal.
- Se ha demostrado la dificultad de actualizar tantos dispositivos a raíz de la vulnerabilidad Krack en WPA
- Se ha probado la facilidad de explorar el tráfico en redes WIFI conocidas.

"No podemos resolver los problemas pensando en la misma manera que cuando los creamos"

Albert Einstein





MUCHAS GRACIAS